(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003296193 A**
(43) Date of publication of application: **17.10.2003**

(51) Int. Cl **G06F 12/14**
G06F 15/00

(21) Application number: **2002099575**
(22) Date of filing: **02.04.2002**

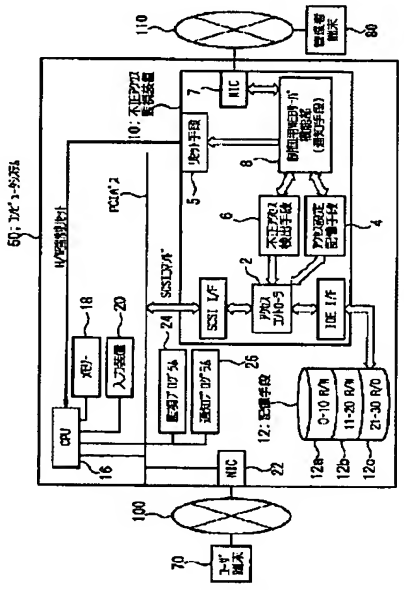
(71) Applicant: **SEIKO INSTRUMENTS INC**
(72) Inventor: **MIYAZAKI HIROSHI**
SHIMIZU HIROSHI

(54) ILLICIT ACCESS MONITORING DEVICE AND METHOD, AND ILLICIT ACCESS MONITORING PROGRAM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an illicit access monitoring device capable of quickly detecting an illicit access to storage means of a computer system while reducing the load on the system.

SOLUTION: This illicit access monitoring device 10 is provided in a computer system 50 having storage means 12a-12c and a control means (CPU) 16. This device is provided with an access controller 2 for managing the access from the CPU to the storage means, an access set storage means 4 for storing the access set (R/W, R/O) of the storage means; an illicit access detecting means 6 for detecting an illicit access to the storage means based on the access set and the access command instructed from the CPU to the access controller; and a reporting means (controlling WEB server function part) 8 for reporting, in the detection of the illicit access, the effect to a manager terminal 80.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－296193
（P2003－296193A）
(43)公開日　平成15年10月17日(2003.10.17)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	12/14	320	G06F	12/14	320A　5B017
		310			310H　5B085
	15/00	330		15/00	330A

審査請求　未請求　請求項の数６　ＯＬ　（全 6 頁）

(21)出願番号　特願2002－99575(P2002－99575)

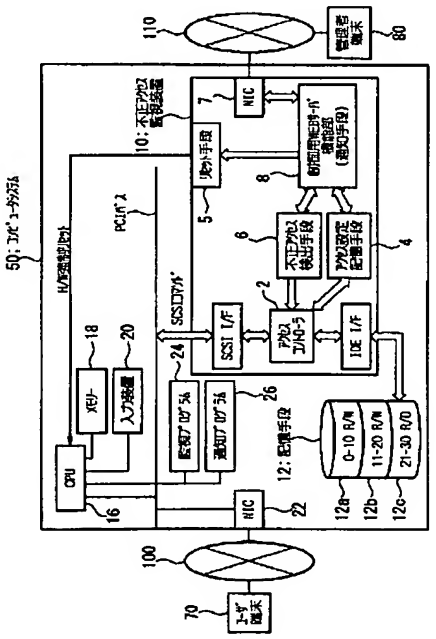
(22)出願日　平成14年４月２日(2002.4.2)

(71)出願人　000002325
セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬１丁目８番地
(72)発明者　宮崎　宏
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツルメンツ株式会社内
(72)発明者　清水　洋
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツルメンツ株式会社内
(74)代理人　100096378
弁理士　坂上　正明

Ｆターム(参考)　5B017 AA08 BA01 CA07
5B085 AE00 BA06 BG02

(54)【発明の名称】　不正アクセス監視装置及び方法、並びに不正アクセス監視プログラム

(57)【要約】
【課題】　コンピュータシステムの記憶手段への不正アクセスを迅速、かつシステムへの負荷を低減して検出できる不正アクセス監視装置を提供する。
【解決手段】　不正アクセス監視装置１０は、記憶手段１２ａ～１２ｃと制御手段（ＣＰＵ）１６とを備えたコンピュータシステム５０に設けられ、ＣＰＵから記憶手段へのアクセスを管理するアクセスコントローラ２と、記憶手段のアクセス設定（Ｒ／Ｗ，Ｒ／Ｏ）を記憶するアクセス設定記憶手段４と、アクセス設定とアクセスコントローラに対してＣＰＵから指示されるアクセスコマンドとに基づき、記憶手段への不正アクセスを検出する不正アクセス検出手段６と、不正アクセスが検出されると、管理者端末８０へ通知を行う通知手段（制御用ＷＥＢサーバ機能部）８とを備える。



1

【特許請求の範囲】
【請求項１】　記憶手段と制御手段とを備えたコンピュータシステムに設けられる不正アクセス監視装置であって、
前記制御手段から前記記憶手段へのアクセスを管理するアクセスコントローラと、
前記記憶手段のアクセス設定を記憶するアクセス設定記憶手段と、
前記アクセス設定と前記アクセスコントローラに対して前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する不正アクセス検出手段と、
不正アクセスが検出されると、所定の通知先へ通知を行う通知手段とを備えたことを特徴とする不正アクセス監視装置。
【請求項２】　前記不正アクセス監視装置は、所定のネットワークを介して管理端末に接続され、
前記通知手段は、前記管理端末に通知を行うことを特徴とする請求項１に記載の不正アクセス監視装置。
【請求項３】　前記通知手段は、前記制御手段に通知を行うことを特徴とする請求項１に記載の不正アクセス監視装置。
【請求項４】　前記通知手段からの通知、又は前記管理端末からの通知を受信して前記制御手段をリセットさせるリセット手段をさらに備えたことを特徴とする請求項１ないし３のいずれかに記載の不正アクセス監視装置。
【請求項５】　記憶手段と、バックアップ用記憶手段と、これらを制御する制御手段とを備えたコンピュータシステムで用いられ、
前記制御手段から前記記憶手段へのアクセスを管理する過程と、
前記記憶手段のアクセス設定を記憶する過程と、
前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、
不正アクセスが検出されると、所定の通知先へ通知を行う過程とを有することを特徴とする不正アクセス監視方法。
【請求項６】　記憶手段と、バックアップ用記憶手段と、これらを制御する制御手段とを備えたコンピュータシステムで実行される不正アクセス監視プログラムであって、
前記制御手段から前記記憶手段へのアクセスを管理する過程と、
前記記憶手段のアクセス設定を記憶する過程と、
前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、
不正アクセスが検出されると、所定の通知先へ通知を行う過程とをコンピュータに実行させることを特徴とする

2

不正アクセス監視プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータシステム内のデータへの不正アクセスを監視するための不正アクセス監視装置及び方法、並びに不正アクセス監視プログラムに関する。
【０００２】
【従来の技術】従来、コンピュータシステム（サーバシステム）への不正アクセスを監視、検出する方法として、以下が知られている。
【０００３】第１の方法は、ネットワーク上を流れるパケットデータを常時監視し、不正なデータパターンや、禁止されたアクセス先が含まれているかを検出する方法である。第２の方法は、サーバのオペレーションシステム（ＯＳ）やアプリケーションが出力するログファイルを定期的に監視し、不正アクセスの結果がログファイルに残っているか否かを検出する方法である。第３の方法は、サーバのファイル内容を定期的に監視し、前回監視時と内容が異なっているか否かを検出する方法である。これらの方法は、いずれもソフトウェアを用いて検出が行われる。
【０００４】
【発明が解決しようとする課題】しかしながら、上記した従来の不正アクセス監視方法の場合、ソフトウェア上で監視処理を行うのでスループットが低く、検出のタイミングが遅いという問題がある。また、サーバシステム内で監視を行う場合、システム自体がハッキングされると監視ができなくなるという問題がある。
【０００５】本発明は、上記した問題点に鑑みてなされたもので、コンピュータシステムの記憶手段への不正アクセスを迅速、かつシステムへの負荷を低減して検出できる不正アクセス監視装置及び方法、並びに不正アクセス監視プログラムを提供することを目的とする。
【０００６】
【課題を解決するための手段】上記した目的を達成するために、本発明の不正アクセス監視装置は、記憶手段と制御手段とを備えたコンピュータシステムに設けられ、前記制御手段から前記記憶手段へのアクセスを管理するアクセスコントローラと、前記記憶手段のアクセス設定を記憶するアクセス設定記憶手段と、前記アクセス設定と前記アクセスコントローラに対して前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する不正アクセス検出手段と、不正アクセスが検出されると、所定の通知先へ通知を行う通知手段とを備えたことを特徴とする。このような構成によれば、制御手段から記憶手段へアクセスしようとする際のアクセスコマンドを取得してアクセス設定と比較するだけでよいので、不正アクセスがあったか否かを迅速、かつシステムへの負荷を低減して検出できる。ま

た、不正アクセスが検出されると所定の通知先へ通知が可能となる。

【０００７】前記不正アクセス監視装置は、所定のネットワークを介して管理端末に接続され、前記通知手段は、前記管理端末に通知を行うようにしてもよい。このようにすると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段の制御を受けない不正アクセス監視装置から外部の管理端末に不正アクセスを通知できる。

【０００８】前記通知手段は、前記制御手段に通知を行うようにしてもよい。このようにすると、コンピュータシステム内で各種の対処を行うことができる。

【０００９】前記通知手段からの通知、又は前記管理端末からの通知を受信して前記制御手段をリセットさせるリセット手段をさらに備えてもよい。このようにすると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段を強制的に終了させることができ、システムの安全が図られる。

【００１０】本発明の不正アクセス監視方法は、前記コンピュータシステムで用いられ、前記制御手段から前記記憶手段へのアクセスを管理する過程と、前記記憶手段のアクセス設定を記憶する過程と、前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、不正アクセスが検出されると、所定の通知先へ通知を行う過程とを有することを特徴とする。

【００１１】本発明の不正アクセス監視プログラムは、前記コンピュータシステムで実行され、前記制御手段から前記記憶手段へのアクセスを管理する過程と、前記記憶手段のアクセス設定を記憶する過程と、前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、不正アクセスが検出されると、所定の通知先へ通知を行う過程とをコンピュータに実行させることを特徴とする。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態について、各図を参照して説明する。図１は、本発明にかかる不正アクセス監視装置１０を含む不正アクセス監視システム全体の一実施の形態を示す構成ブロック図である。この不正アクセス監視システムは、Ｗｅｂサーバ等からなるコンピュータシステム５０と、本発明の不正アクセス監視装置１０とから構成される。不正アクセス監視装置１０は、例えばＰＣＩ(Peripheral Component Interconnect)ボード等からなり、コンピュータシステム５０のＰＣＩスロットに挿入され、ＰＣＩバスに接続されて動作するようになっている。

【００１３】コンピュータシステム５０は、インターネット等の外部ネットワーク１００を介してユーザ端末７０に接続され、ユーザはユーザ端末７０からコンピュータシステム５０内の各種データ（コンテンツ）を閲覧したり、データの更新を行えるようになっている。又、不正アクセス監視装置１０は、イントラネット等の内部ネットワーク１１０を介して管理者端末８０に接続され、管理者は管理者端末８０から不正アクセス監視装置１０とやりとりを行う。各ネットワークとしては、専用回線、ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等を用いてもよい。

【００１４】コンピュータシステム５０は、各種データを記憶する記憶手段１２（１２ａ～１２ｃ）、ＣＰＵ（制御手段）１６、所定のメモリ１８、キーボード等の入力装置２０、外部ネットワーク１００に接続される通信インターフェース（ＮＩＣ）２２を備えている。また、ＣＰＵ１６によって動作する監視プログラム２４、通知プログラム２６を備えている。

【００１５】ここで、この実施形態では、ハードディスク等の記憶媒体からなる記憶手段１２が複数のパーティション１２ａ～１２ｃに分割され、それぞれデータが記憶されている。各パーティションはそれぞれアクセス設定がされている。アクセス設定とは、記憶手段へのアクセス方法の設定をいい、例えば記憶手段の読出しのみを許可して書込みを禁止するＲ／Ｏ(Read Only)、記憶手段の読出しも書込みも許可するＲ／Ｗ(Read Write)がある。この実施形態では、記憶手段１２のうち、セクタアドレス０～１０に相当するパーティション１２ａがＲ／Ｗに、セクタアドレス１１～２０に相当するパーティション１２ｂがＲ／Ｗに、セクタアドレス２１～３０に相当するパーティション１２ｃがＲ／Ｏに、それぞれ設定されている。

【００１６】記憶手段１２は、不正アクセス監視装置１０を介してＣＰＵ１６と接続され、不正アクセス監視装置１０からアクセス制御されるようになっている。なお、上記実施形態では、１つの記憶媒体（例えばハードディスク）内の領域をパーティション分割したが、別個の記憶媒体からなる複数の記憶手段としてもよい。

【００１７】本発明の不正アクセス監視装置１０は、アクセスコントローラ２、アクセス設定記憶手段４、リセット手段５、不正アクセス検出手段６、通知手段（制御用ＷＥＢサーバ機能部）８、内部ネットワーク１１０に接続される通信インターフェース（ＮＩＣ：Network Interface Controllar）７、図示しないメモリ等を備えている。アクセスコントローラ２、アクセス設定記憶手段４、リセット手段５、不正アクセス検出手段６、通知手段８、通信インターフェース７は、例えばプリント基板上に搭載されるＣＰＵ等から構成される。

【００１８】アクセスコントローラ２は、ＣＰＵ１６とＰＣＩバスを介して接続されるとともに、記憶手段１２と接続され、ＣＰＵ１６から記憶手段１２へのアクセスを管理する。なお、ＣＰＵ１６との接続は例えばＳＣＳＩ(Small Computer System Interface)インターフェー

スが用いられ、記憶手段１２との接続は例えばＩＤＥ(Integrated Device Electronics)インターフェースが用いられる。

【００１９】アクセス設定記憶手段４は、記憶手段１２のアクセス設定を記憶する。この実施形態では、各パーティション１２ａ～１２ｃ毎のアクセス方法の設定、つまり、パーティション１２ａに該当するセクタアドレスがＲ／Ｗに、パーティション１２ｂのセクタアドレスがＲ／Ｗに、パーティション１２ｃのセクタアドレスがＲ／Ｏに、それぞれ設定されていることが記憶されている。アクセス設定記憶手段４へのデータの登録は、管理者端末８０からＮＩＣ７、通知手段８を介して行われ、ＣＰＵ１６からの指示によっては登録や更新ができないようになっている。なお、アクセス設定記憶手段４をディップスイッチ等で構成し、アクセス設定を管理者が手動で行うようにしてもよく、その他のハードウェアスイッチで構成しても勿論よい。

【００２０】不正アクセス検出手段６は、上記アクセス設定と、アクセスコントローラ２に対してＣＰＵ１６から指示されるアクセスコマンドとに基づき、記憶手段１２への不正アクセスを検出する。アクセスコマンドは次のようなものである。まず、ユーザ端末７０又は入力装置２０から記憶手段１２への読出し（書込み）要求をＣＰＵ１６が受信する。ＣＰＵ１６はこの要求をＳＣＳＩ形式の読出し（書込み）コマンドに変換してアクセスコントローラ２に送信し、不正アクセス検出手段６はアクセスコントローラ２からこのコマンドを取得する。

【００２１】通知手段（制御用ＷＥＢサーバ機能部）８は、不正アクセス検出手段６から不正アクセス検出を受信すると、所定の通知先へ通知を行う。この実施形態では、通知手段８はＮＩＣ７に接続され、内部ネットワーク１１０を介して管理者端末８０へ不正アクセスがあった旨を通知したり、リセット手段５を介してＣＰＵ１６へ信号を通知する。なお、リセット手段５はＣＰＵ１６をハードウェア上で強制終了させるリセット信号を生成し、ＣＰＵ１６はリセット信号を通知されるようになっている。

【００２２】通知手段８は、また、例えばＨＴＭＬ等で記述されたＷｅｂページを格納しており、管理者端末８０にこのＷｅｂページを各種の設定画面として表示させる制御用ＷＥＢサーバ機能を有している。これにより、管理者は、記憶手段１２のアクセス設定を画面上で行い、その設定情報は通知手段８の制御によりアクセス設定記憶手段４に登録される。また、管理者端末８０からは、その他の例えば記憶手段１２のパーティション設定等を行うこともできる。

【００２３】なお、通知手段８を介さずにＣＰＵ１６へ不正アクセスがあった旨を通知することもできる．この場合、不正アクセス検出手段６からアクセスコントローラ２へ不正アクセス検出が送信されると、アクセスコントローラ２は所定のＳＣＳＩコマンドを生成してＣＰＵ１６へ送信する。ＣＰＵ１６はこのコマンドを受信すると、監視プログラム２４、通知プログラム２６を順次起動し、後述する処理を行う。

【００２４】次に、図２を参照して、（コンピュータシステム５０の）ＣＰＵ１６、不正アクセス監視装置１０、管理者端末８０間で行われる処理フローを説明する。

【００２５】この図において、まず、管理者端末８０から不正アクセス監視装置１０へ接続し、設定画面上で記憶手段１２の書込み禁止の設定（アクセス設定）を行う（ステップＳ１）。この場合、設定がされない状態では書込み可能（Ｒ／Ｗ）とし、書込み禁止を設定するとＲ／Ｏ状態になるようにしてもよい。通知手段８は、アクセス設定記憶手段４にこの設定を記憶させる（ステップＳ３）。

【００２６】次に、ＣＰＵ１６から記憶手段１２の書込みコマンド（ＳＣＳＩ）が送信されると（ステップＳ１０）、アクセスコントローラ２はそのコマンドを不正アクセス検出手段６へ送信する（ステップＳ１２）。不正アクセス検出手段６は、コマンドを受信すると、アクセス設定記憶手段４に記憶された設定を読み取り（ステップＳ１４）、不正アクセスの判定を行う（ステップＳ１６）。

【００２７】判定は、例えば以下のようにして行われる。まず、不正アクセス検出手段６は、コマンドに含まれる書込み対象領域を解析する。この領域は、記憶手段がパーティション分割されている場合、対象となるパーティションのセクタアドレスである。次に、不正アクセス検出手段６は、解析した書込み対象領域とアクセス設定記憶手段４の設定とを比較し、その書込み対象領域（セクタアドレス等）が書込み禁止（Ｒ／Ｏ）に設定されている場合は不正書込み（不正アクセス）検出と判定する。なお、この実施形態では、不正アクセス検出の有無に関わらず、書込み禁止領域への書込み処理自体は実行される。

【００２８】以上のように、ＣＰＵ１６から記憶手段１２へアクセスしようとする際には、アクセスコマンドが必然的にアクセスコントローラ２に送信される。従って、不正アクセス検出手段６は、アクセスコマンドを取得してアクセス設定と比較するだけでよく、不正アクセスがあったか否かを迅速、かつシステムへの負荷を低減して検出できる。特に、ハードウェア上でアクセスコマンドとアクセス設定の比較を行えば、より迅速かつ軽負荷で処理が行える。

【００２９】このようにして不正書込みが検出されると、不正アクセス検出手段６は、不正検出を通知手段８やアクセスコントローラ２へ通知する（ステップＳ１８、Ｓ２０）。通知手段８は、ステップＳ１８で通知を受信すると、管理者端末８０へ不正書込み検出を通知す

る（ステップＳ２２）。これにより、管理者は不正書込みがあったことを知る。

【００３０】一方、アクセスコントローラ２は、ステップＳ２０で通知を受信すると、所定のＳＣＳＩコマンドを生成してＣＰＵ１６へ送信する（ステップＳ２４）。このＳＣＳＩコマンドは、ステップＳ１０で受信した書込みコマンドの情報を付加している。

【００３１】ＣＰＵ１６は、コマンドを受信すると、監視プログラム２４、通知プログラム２６を順次起動する（ステップＳ２６、Ｓ２８）。監視プログラム２４は、ＳＣＳＩコマンドに付加された情報を参照して、書込みを行ったプロセスＩＤ、ユーザＩＤ等を特定し、書込み元が正規の者であるか否かを判定する。この判定は、例えば正規のシステム管理者の場合、書込み禁止領域にも所定の情報を書き込むことがあるのを想定している。そして、正規のシステム管理者でない者による不正な書込みであると判定すると、監視プログラム２４は通知プログラム２６に対して通知を指示し、通知プログラム２６は所定の通知先（管理者端末８０等）へ不正書込みを通知する（ステップＳ３０）。

【００３２】本発明は上記した実施形態に限られない。例えば上記実施形態ではステップＳ１６で、書込み禁止領域に対して書込みコマンドが発行されると不正アクセスと判定したが、書込み可能領域に対して書込みコマンドが発行された場合でも不正アクセスと判定してもよい。

【００３３】前記図１の場合を例とすると、記憶手段１２の各パーティションの読み書き状態（Ｒ／Ｗ、Ｒ／Ｏ）をアクセス設定とする代わりに、各パーティションに対応するセクタアドレスをアクセス設定とする。つまり、パーティション１２ａに相当するセクタアドレス０～１０は、Ｒ／ＷかＲ／Ｏに関わらず書込み禁止領域であるとみなす。従って、セクタアドレス０～１０への書込みコマンドがあると不正アクセスと判定し、管理者端末８０やＣＰＵ１６へ通知する。ＣＰＵ１６は、前述のように監視プログラムを起動し、不正アクセスと判定した者が正規のシステム管理者か否かをさらに判定する。このようにすると、セクタアドレス０～１０に管理用のデータを記憶させた場合に有効である。つまり、セクタアドレス０～１０には通常のユーザはアクセスしないが、管理者によるデータ更新のために書込み可能としておく必要がある。そして、書込みが行われた場合は仮に不正アクセスと判定し、その書込みが正規の管理者によると判明すれば不正アクセスでなかったものとし、不正者による場合はただちに対処することができる。

【００３４】なお、本発明の不正アクセス監視装置は、コンピューターと、通信装置等の各種周辺機器と、そのコンピューターによって実行されるソフトウェアプログラムとによって実現することができ、上記システム内で実行されるソフトウェアプログラムは、コンピューター読み取り可能な記憶媒体あるいは通信回線を介して配布することが可能である。また、本発明の不正アクセス監視装置は、サーバシステムの他、パーソナルコンピュータ、ルータ、ファイアウォール等に設けることができる。

【００３５】

【発明の効果】以上説明したように、本発明によれば、制御手段から記憶手段へアクセスしようとする際のアクセスコマンドを取得してアクセス設定と比較するだけでよいので、不正アクセスがあったか否かを迅速、かつシステムへの負荷を低減して検出できる。また、不正アクセスが検出されると所定の通知先へ通知が可能となる。

【００３６】本発明において、不正アクセス監視装置が所定のネットワークを介して管理端末に接続され、通知手段が管理端末に通知を行うようにすると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段の制御を受けない不正アクセス監視装置から外部の管理端末に不正アクセスを通知できる。

【００３７】本発明において、通知手段が制御手段に通知を行うようにすると、コンピュータシステム内で各種の対処を行うことができる。例えば、不正アクセスと判定した者が正規の管理者であるか否かの２次的な判定を行うことができる。

【００３８】本発明において、通知手段からの通知、又は管理端末からの通知を受信して制御手段をリセットさせるリセット手段をさらに備えると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段を強制的に終了させることができ、システムの安全が図られる。

【図面の簡単な説明】

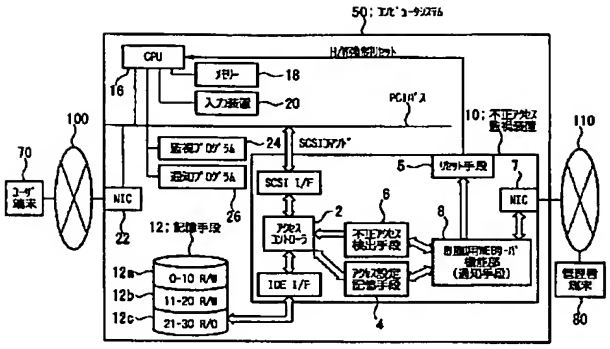
【図１】　本発明の不正アクセス監視装置を含む不正アクセス監視システム全体の構成を示すブロック図である。

【図２】　ＣＰＵ、不正アクセス監視装置、管理者端末間で行われる処理のフローを示す図である。

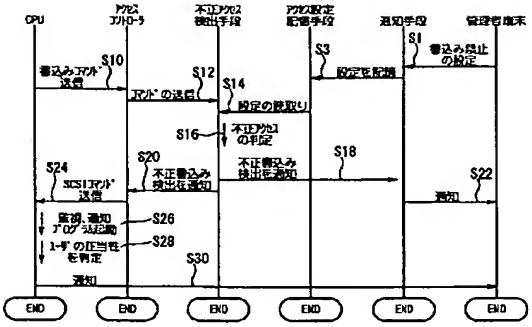
【符号の説明】

２	アクセスコントローラ
４	アクセス設定記憶手段
６	不正アクセス検出手段
８	通知手段（制御用ＷＥＢサーバ機能部）
１０	不正アクセス監視装置
１２ａ～１２ｃ	記憶手段
１６	制御手段（ＣＰＵ）
５０	コンピュータシステム
８０	管理者端末

【図１】


50; エンピュータシステム
CPU
メモリー
18
入力装置
20
16
PCIバス
100
70
ユーザ端末
NIC
22
監視プログラム
24
SCSIコマンド
10; 不正アクセス監視装置
110
SCSI I/F
リセット手段
5
7
NIC
通知プログラム
26
12; 記憶手段
アクセスコントローラ
2
6
8
不正アクセス検出手段
自動切断機能付ハブ装置（通知手段）
アクセス設定記憶手段
IDE I/F
12a
12b
12c
0-10 R/W
11-20 R/W
21-30 R/O
4
管理者端末
80

【図２】


CPU
アクセスコントローラ
不正アクセス検出手段
アクセス設定記憶手段
通知手段
管理者端末
S1
書込み禁止の設定
S3
設定を記憶
S10
書込みコマンド送信
S12
コマンドの送信
S14
設定の読取り
S16
不正アクセスの判定
S18
S20
不正書込み検出を通知
S22
通知
S24
SCSIコマンド送信
S26
監視、通知プログラム起動
S28
ユーザの正当性を判定
S30
通知
END
END
END
END
END
END